Cryptographic Protocols for Secure Electronic Commerce(Abstract_要旨)

AUTHOR(S):

Mitsunaga, Takuhou

（ 続紙 1 ）

京都大学	博士（情報学）	氏名	満永　拓邦
論文題目	Cryptographic Protocols for Secure Electronic Commerce (安全な電子商取引のための暗号プロトコル)		

（論文内容の要旨）

本論文は，暗号理論に基づき多角的な観点から安全な電子商取引の実現を目指すものである．本論文では，電子商取引を行うにあたって必要な手順を，(1)電子商取引に関するルールの合意形成，(2)電子商取引の設計，(3)アプリケーションとしての実現，という３層に分け，各層における現在の課題と解決を図るアプローチを採用している．そのうえで、各層において暗号理論を用いた安全なモデルを示し，セキュリティ上の観点から優れた，一貫したモデルの構築を目指している．それらを通じて利用者にとって安全な電子商取引の実現を試みている．

本論文は，全6章からなる．

第 1 章では序論として，インターネットの普及に伴い電子商取引が発展していることについて既存の調査結果を引用しつつ解説している．併せて，電子商取引が発展する一方で，サイバー攻撃による被害が深刻化していることに触れ，安全な電子商取引に関する研究を行う意義，背景，目的について記述している．また本論文で提案する３層のアプローチおよび各層での課題について明らかにしている．

第 2 章は，本論文を構成するうえで基礎となる暗号理論やゲーム理論について解説している．

第 3 章は，暗号理論を用いた安全な電子商取引の設計について論じている．安全な電子商取引の一例として，実社会において広く普及しているオンラインオークションのセキュリティについて取り上げ，オークションにおけるセキュリティ上の課題である，主催者によるオークション結果の改ざんについて説明するとともに，落札者以外のプレイヤーの入札額に対する秘匿性およびオークション結果に対する検証可能性を担保するセキュアオークションプロトコルについて詳細に解説している．まず，単一の財に対し最高入札者が落札者，最高入札価格が落札価格となる第一価格オークションについて説明している．その後，最高入札者が落札者，第二最高入札価格が落札価格となる第二価格オークションを紹介し，それぞれの方式についてセキュアオークションプロトコルについて述べるとともに，BGN 暗号が持つ加法準同型性と乗法準同型性の特性をビットスライスと呼ばれる手法に適用した効率的なセキュアオークションプロトコルを提案している．また，これらの提案手法が既存研究と比較して効率的であることを示している．更には，M 個の単一種類の財に対して，上位 M 人の高額入札者が落札者，(M+1)番目の入札価格が落札額となる M+1 価格オークションについて説明し，M+1 価格オークションにおけるセキュアオークションプロトコルも提案し

ている．また，提案方式により正しく出力されること，また既存方式と比較して効率的であることを証明している．

第 4 章では，ゲーム理論に対し暗号理論を応用することにより，電子商取引に関するルールの合意形成を図る．種々の複雑な電子商取引を効率的に実現するためのメカニズムについて暗号とゲーム理論の観点から既存研究の説明を行いつつ，複数の関係者における合意形成についてまとめている．併せて電子商取引を行うにあたって様々なルールを事前に定める必要性と，この章で述べられる利害調整のメカニズムによる電子商取引に関する合意形成の重要性に言及している．既存研究において、ゲームの事前段階での調整メカニズムに暗号理論を用いることで，信用できる第三者の存在なしに相関均衡が達成したことを説明している．また，複数のプレイヤーが結託し，事前の調整メカニズムにて定められた均衡から逸脱する場合に，それらのプレイヤーに対し罰則を与えるパニッシュメント戦略が提案されていることを述べている．更にパニッシュメント戦略が存在したとしても，事前の調整から逸脱しないプレイヤーも，自己の利益を求め，パニッシュメント以外の戦略を選択する例を示し，パニッシュメント戦略の新たな定義を提案している．

第 5 章では，電子商取引をシステム上で実装した際のセキュリティ上の課題を解消するため，Web 環境における安全な認証方式を提案している．多くの電子商取引は，Web サイトを利用して実現されていることに触れ，Web 環境における認証技術の社会的な重要性を解説している．また，Web サービスにおけるユーザ認証としてアカウント登録時に設定される ID とパスワードを用いるパスワード認証方式が一般的に利用されている現状を述べ，それに起因するパスワードリスト型攻撃などの新しい攻撃手法および Anomaly 検知などの既存の対策について説明している．パスワード認証方式に代わる，安全性を向上させた認証方式の必要性を説明するとともに，HTML5 で導入された Web Storage という機能を用いて，パスワードリスト型攻撃への耐性を持つ公開鍵認証方式に基づく Web サービス認証方式を提案している．

最後に，第 6 章は結論であり，研究の背景，目的を踏まえたうえで，本論文で採用した３層アプローチにおいて各層での課題が解決されたことを示し，全体として一貫したモデルが構築できたことについて説明している．また，それにより達成された成果の概要をまとめている．

（続紙 ２ ）

（論文審査の結果の要旨）

インターネットの普及により，オンラインオークションやインターネットバンキングなど電子商取引は身近な存在となっている．一方で，インターネット上において，コンピュータやネットワークに不正に侵入し，データの破壊や改ざん，情報窃取，システム停止などの損害を与えるサイバー攻撃が後を絶たず，安全な電子商取引の実現に向けた研究の意義は大きい．

本論文では，電子商取引における様々な問題に対して暗号理論を用いて多面的な解決を試みている。これら一連の研究は，安全性やプライバシを保持した電子商取引を実現することに寄与するものである．安全な電子商取引を実現するうえで，各論で分析された具体的な研究は，いずれも重要なテーマである．例えば，第 3 章において，社会において広く普及している電子商取引であるオークションプロトコルを安全かつ効率的に実現していることや，第 4 章において，電子商取引などの複数の利害関係者におけるメカニズムを分析したうえで，新たな定義にもとづく手法を提示していることは，安全な電子商取引のための社会基盤確立に資する内容となっている．また第 5 章での Web 環境における認証の研究においては，提案方式が安全であるという理論的な分析だけではなく，具体的な実装まで示されている点も評価できる．さらに提案方式の安全性も十分に説明がされており，実社会における Web アプリケーションのセキュリティに寄与するものであると認められる．このように，本論文は電子商取引を行う上で必要となる関係者間の合意形成から安全性の電子商取引の設計，実装まで網羅的な論点を取り扱っており，各論点において暗号理論を用いた解法を示し，セキュリティ上の観点から優れた，一貫した電子商取引のモデルを構築している．

本論文の研究成果は、実社会におけるサイバー攻撃の被害の軽減に資するもので，学術上、実用上寄与するところが少なくない。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。また、平成 28 年 2 月 12 日，論文内容とそれに関連した口頭試問を行った結果合格と認めた．